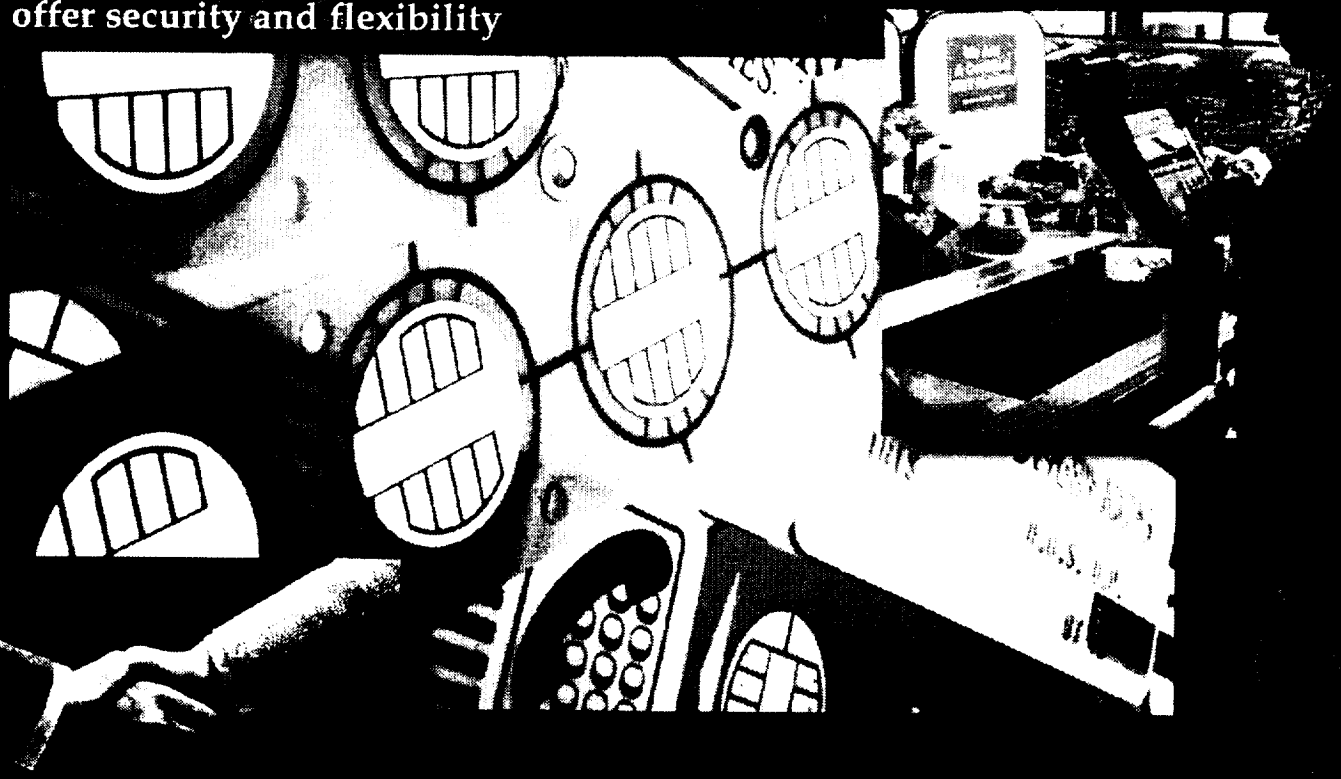
Table of Contents

Electronic Benefit Transfer (EBT) Guide to Functional Specifications for Smartcards for Off-Line EBT Applications

USDA • Food and Consumer Service • 3101 Park Center Drive • Alexandria • VA • 22302

Smartcard operating systems offer security and flexibility

Staged transactions deliver benefits right in the store



ISO, EMV and USDA specifications work together

EBT

Table of Contents

Electronic Benefit Transfer (EBT) Guide to Functional Specifications for Smartcards for Off-line EBT Applications

Contract No. 53-3198-3-023

Evaluation of the SmartCard EBT Demonstration in Wyoming

April 1996

Prepared for

Julie Kresge
U.S. Department of Agriculture
Food & Consumer Service
3101 Park Center Drive
Alexandria, Virginia 22302

Prepared by

Joseph Schuler
The Schuler Consultancy
with
Abt Associates Inc.
55 Wheeler Street
Cambridge, Massachusetts 02138

TABLE OF CONTENTS

Acknowledgements i

Introduction 1

Smartcard Functioning 4

Suggested Functional Requirements for EBT 8

Glossary 13

Overview of the PayEase[S.M.] EBT System 15

ACKNOWLEDGEMENTS

The Food and Consumer Service wishes to thank Joseph Schuler, The Schuler Consultancy, for his expert guidance in seeking industry views on ways to functionally define requirements for integrated circuit cards, or "smartcards," in EBT systems for the Food Stamp Program and the Special Supplemental Nutrition Program for Women, Infants, and Children (WIC).

C. Sidney Price, Stored Value Systems, and J. Terry Williams, manager for Wyoming's EBT project, set aside busy schedules to share essential insights based on their experiences in Wyoming.

Thanks go to the leaders of industry and government who helped shape guidance to states through their suggestions on draft functional specifications for off-line EBT. We sincerely appreciate the willingness of the following individuals to generously donate their time and expertise to this effort:

Philip Lee, ASI
Kymberly Wiggin, DataCard
Cassie Metzger, Diebold, Inc.
Henry Dreifus, Dreifus Associates, Ltd.
Paul Coenen, Electronic Strategy Associates, Inc.
John Esser, G&D America
Gilles Lisimaque, Gemplus Card International
William Lane, HYPERCOM, Inc.
John Shipley, JIL Information Systems
Peter Thorp, 3M
Xavier Delaroue, Micro Card Technologies, Inc.
Kip Wheeler, Personal Computer Card Corp.
Bob Gilson, Smart Card Forum
Michael Noll, U.S. Office of the Assistant Secretary of Defense, C3I
Robert Warner, NIST

Thanks to Glenn Edelman, EFT Association ; John Moore, Federal Smart Cards User's Group; and Ben Miller, CardTech SecurTech, who facilitated communications of draft specifications to a wide variety of stakeholders surrounding the smart card industry.

Finally, a special thank-you is owed to the many individuals who have made possible joint efforts by Europay, MasterCard, and Visa (EMV) in defining the needs of the financial

sector with regard to smart card technology. The EMV specifications for both cards and terminals make it possible for the current guidance to build upon their solutions and to expand into newly-charted territory.

INTRODUCTION

The Food and Consumer Service (FCS) of the U.S. Department of Agriculture is currently exploring the use of off-line technology to deliver benefits electronically in the Food Stamp Program (FSP) and the Special Supplemental Nutrition Program for Women, Infants, and Children (WIC). Demonstration projects now exist in Ohio for the FSP, and in Wyoming for both the FSP and WIC.

Although electronic benefit transfer (EBT) is now becoming fairly widely used in the FSP, the predominant approach to date has relied on on-line technology. In the on-line approach, each food purchase at a grocery store must be authorized by a central computer that maintains an "account balance" for all recipients. This requires on-line communication between the point of sale (POS) terminal and the central computer before the purchase can be completed. Recipients in this system are issued magnetic-stripe cards, similar to bank ATM cards, whose magnetic stripe contains information identifying the recipient and the account.

The off-line approach allows a transaction to be completed at the POS without immediate communication with the central computer. The account balance information is maintained within the recipient's EBT card. Purchases are authorized and the balance is updated by an interaction between the card and the POS terminal, and reported later to the central computer.

The off-line EBT approach requires a card with greater memory and processing capacity than the on-line approach. The applications to date have used integrated circuit cards, or "smartcards." Such cards are also being widely tested for a variety of uses in commercial electronic financial transactions, and many observers believe that smartcards will be in common use for consumer debit and credit transactions within the near future.

An important obstacle to using smartcards in broad EBT or commercial applications is the current incompatibility of cards produced by different manufacturers. This means that an EBT system built around a particular card might be unable to use cards made by other manufacturers, and would probably not be able to share retailer POS terminals with potential commercial EFT users. These factors tend to limit the applicability of the off-line EBT approach and increase its costs.

Smartcard Functions Guide

To move toward increasingly compatible and useful smartcards, FCS initiated an effort to define a set of functional requirements that smartcards should meet for EBT purposes. This effort was carried out at about the same time as a major effort within the financial industry to develop industry specifications for smartcard functioning in financial transactions.

The International Organization for Standardization (ISO) has been publishing the standards for integrated circuit cards with contacts since 1987. The ISO 7816 standard has been released in six parts.[1] The standard covers the physical characteristics, dimensions, and locations of the contacts, electronic signals and transmission protocols, and data exchange messages used for smartcards. The standard is quite general, and can be applied to various applications, such as communication, transportation, access control, payment systems, or health care.

Europay, MasterCard and VISA formed an alliance to write specifications for debit and credit functions using smartcards in Electronic Payment Systems (EPS).[2] This set of specification is called Integrated Circuit Card Specifications for Payment Systems. It was first released in 1994 and was followed by further revisions June 30, 1995 (version 2.0). Another set of revisions to this specification is expected in June 1996.

VISA, MasterCard, and other firms have been independently developing specifications for creation and use of electronic purse (debit type) applications on smartcards. This application

---

[1] ISO 7816: Identification Cards—Integrated Circuit(s) Cards with Contacts
- Part 1: Physical Characteristics (July 1, 1987)
- Part 2: Dimensions and Location of the Contacts (May 15, 1988)
- Part 3: Electronic Signals and Transmission Protocols (December 1, 1994)
- Part 4: Interindustry Commands for Interchange (September 1, 1995)
- Part 5: Numbering System and Registration Procedure for Application Identifiers (Jun 6, 1994)

[2] Integrated Circuit Card Specifications for Payment Systems
- Part 1: Electromechanical Characteristics, Logical Interface, and Transmission Protocols (version 2.0, June 30, 1995)
- Part 2: Data Elements and Commands (version 2.0, June 30, 1995)
- Part 3: Transaction Processing (version 2.0, June 30, 1995)

Integrated Circuit Card Terminal Specification for Payment Systems (version 1.0, June 30, 1995)

specification is called Stored Value Card Specification.[3] Currently, some firms are writing versions of this specification while others are testing their specification. The specifications are proprietary to the authoring firms.

The EBT functional requirements in this Guide were developed with the financial industry specifications in mind, assuming manufacturers will meet those industry specifications. Ideally, all smartcard manufacturers would produce cards meeting both the financial industry specifications and these EBT specifications, which would maximize compatibility and limit the special development work needed for off-line EBT applications.

This Guide presents the functional requirements for EBT application of smartcards in order to facilitate discussion between states and the smartcard industry as they seek to develop new EBT systems. It begins with a brief description of the way that smartcards work and how they perform EBT functions, and then presents the recommended functional requirements. The Guide includes a glossary of some of the terms used, and an overview of the off-line smartcard system used in Ohio and Wyoming.

[3] VISA Rechargeable Card Specification (version 1.1, February 15, 1995)
VISA CAD/Service Payment Terminal Specification (version 2.2, February 17, 1995)
VISA Non-rechargeable Card Specification (version 1.2, 1995)
VISA Concentration Point Specification (version 2.1, March 22, 1994)

SMARTCARD FUNCTIONING

The introduction of operating systems for personal computers, such as MS-DOS®,[4] allowed software developers to focus on their application instead of computer and peripheral device technical requirements. Programmers no longer had to write hardware-specific programs and routines dedicated to a certain manufacturer's components. Operating systems made application software more portable, easier to upgrade, and more affordable. For example, it is not necessary to rewrite the file access portion of an application to take advantage of a new, higher-capacity, higher-performance disk drive. Operating systems take care of allocating disk space and keeping track of the ***physical*** address (cylinders and tracks) where directories and files are stored. Application developers and users can therefore assign ***logical*** directory and file names, which are much more meaningful.

Card or Chip Operating Systems (COS) are intended to accomplish much the same functionality for smartcards that MS-DOS has done for personal computers. Although most manufacturers and some third-party vendors have developed chip operating systems for their smartcards, an industry standard COS has not yet emerged. Each COS is a proprietary product that is incompatible with the others, except for some very basic ***Reset*** and ***Answer-to-Reset*** start-up procedures defined by the International Organization for Standardization (ISO).

The lack of a standard or agreement for a common chip operating system makes the development of multiple-vendor smartcard applications very difficult. Special care must be exercised in order to use smartcards and terminal/Card Acceptor Devices (CADs) manufactured by different vendors. Just as Apple- and IBM-compatible computers cannot easily read each other's files, CADs cannot easily read and write smartcards from different manufacturers. There is no standard COS, nor anything as common as Microsoft's MS-DOS in the smartcard industry. With the exception of the *Integrated Circuit Card Specifications for Payment Systems* development by Europay, MasterCard, and Visa (EMV), few efforts have been launched to provide a common set of financial application commands.

[4] MS-DOS is a registered trademark of Microsoft Corporation.

Smartcard Functions Guide

VISA International is making efforts to define specifications for a Stored Value Card System (SVCS) using various card operating systems. These specifications were initially released in 1995, and the newer version is expected in June 1996.

The EBT functional requirements in this Guide were developed with the financial industry specifications in mind, assuming card and terminal manufacturers will meet those industry specifications. Ideally, all smartcard manufacturers would produce cards meeting both financial industry specifications and these EBT specifications, which would maximize compatibility and limit the special development work needed for off-line EBT applications. Because the smartcard industry is still rapidly developing, the following discussion and suggested functional requirements for EBT are expected to need updating as innovation and expansion of smartcard capabilities continue.

What Is a COS?

A COS is a software program that resides in the smartcard chip. It manages the hardware and data resources of the chip and facilitates use of those resources through a set of commands and a file structures. The COS (sometimes referred to as the "mask") is permanently programmed into the chip when the silicon chip is manufactured.

File Structure

Smartcard operating systems manage data at the file level. They allow files to be created, opened, read, written, closed, erased, and deleted. The application may define Read, Write, and Update protection, file type, and a file identifier when files are created. Three types of files are normally supported by a COS. They are:

- ***Linear fixed length files***, which contain records of all the same number of bytes or bits;
- ***Linear variable length files***, which may contain records of variable length. They usually have a specified maximum length and some type of header data in each record that designates its length; and

- ***Cyclic files***, files of either fixed or variable length records where the last record points to the first record, thereby creating a never-ending circle. Cyclic files are ideally suited to storing a copy of, for example, the last ten transactions.

File identifiers eliminate the need for terminal application programmers to be concerned with the physical layout of memory. The allocation of files is dynamic, meaning that a new file can be created at any time during the life of the card once the proper authorization has been presented. The file is usually the lowest element for which access protection is provided by a COS. One or more secret codes, or keys, may have to be presented before a file can be opened, read, written, or updated, depending on the access conditions established when a file is created. Three consecutive incorrect key presentations may lock the application or card to protect against unauthorized access.

Commands

In order to control file access and perform calculations, the COS needs to be supplied with a logical sequence of instructions to follow. These instructions, or commands, are issued to the card by an application program residing in a host computer or smartcard terminal. For each command sent to the COS, there is an appropriate response sent back to the host or terminal. Therefore, a dialogue of commands and responses goes back and forth between the application program and the COS to carry out even the simplest procedure. For example, the following steps or similar steps are required to perform an off-line payment or EBT transaction—all under control of the terminal or host application program:

- Terminal/card/PIN authentication (optional);
- Terminal submits the proper application key to the card;
- The account balance is read from the card into the terminal's memory;
- The balance now in the terminal is credited or debited, and then the updated balance is rewritten back into the card.

Under this scheme, each terminal must contain the logic and keys required to both credit ***and*** debit accounts contained in a card, even if the terminal is a debit-only terminal such as a vending machine. This means that every terminal has logic and keys that could be used to modify cards fraudulently, which creates a potentially high-risk security environment.

Several smartcard manufacturers have each developed a COS specifically designed for the electronic payments industry. These new operating systems were generally implemented by layering electronic payment functions on top of the manufacturer's existing proprietary operating systems. Payment chip operating systems have built-in logic to perform Debit, Credit, Read Balance, and Electronic Signature functions with less dialogue between the card and the terminal than was previously required.

The approach with these new chip operating systems is totally different than their predecessors. The account balance contained in the card's memory is read, updated, and rewritten under control of the software in the card, not terminal application software. Terminal application software is never given direct access to read or write, credit or debit the card's account information. Payment chip operating systems also divide debit and credit into two separate functions. The following steps are required to perform an off-line debit (purchase) transaction using one of these new operating systems:

- Terminal/card/PIN authentication (optional);
- A session key is established;
- Terminal submits the proper debit application key to the card;
- Terminal submits the transaction amount;
- The payment COS: (1) checks that the balance is greater than or equal to the debit amount, (2) computes the new balance, (3) computes message authentication code (MAC) and (4) sends the MAC to the terminal.

Debit terminals using a payment COS only have the keys and logic needed to submit purchase amounts to the card. They have no keys or logic for credit transactions, and they never have direct access to information in the card's memory. Therefore, the terminals can be less sophisticated while affording higher levels of speed and security than more traditional chip operating systems. This is turn tends to reduce the cost of the terminals and improve the business case for equipping retailers.

SUGGESTED FUNCTIONAL REQUIREMENTS FOR EBT

Smartcards for EBT applications should provide the functionality of a payment COS. In addition, to the extent practical, they should provide the functionality defined below and comply with the physical and logical interface requirements provided for in the Europay, MasterCard, and Visa (EMV) specification. Terminal devices for EBT should also comply with the physical and logical interface requirements provided for in the EMV terminal specification.

Indivisible Operations

Whenever possible, the COS should support posting transactions to cards in a single indivisible operation between the CAD and card.

> ***Reason:*** Several commands and responses must be exchanged between a CAD and a smartcard to complete most transactions using today's off-the-shelf card operating systems. Reducing the transaction dialogue to a single command, such as those available from some manufacturers for stored value card programs, would greatly simplify terminal-to-card processing and would possibly enhance overall security and transaction integrity.

Avoid Duplicate Postings

The COS should provide the ability to prevent duplicate posting of identical transactions to a card.

> ***Reason:*** Transactions used to credit (and sometimes debit) an account balance carried in an EBT recipient's card are created by the host computer system. In current off-line systems, the information is then transmitted on-line to up to three merchant locations, where it awaits arrival of the card. A "staged" transaction is applied to the card off-line the first time the card is presented at one of the three merchant locations. Once a staged transaction is applied at one location it must not be applied again; otherwise, double or even triple posting of the same transaction would be possible. Therefore, a mechanism must be implemented to assure that a staged transaction is only applied once to a card, even if the card is presented at all multiple locations where the credit information is stored.

Linking to History File

A general purpose mechanism for defining and linking applications to a transaction history file should be provided.

> ***Reason:*** When multiple benefit programs are implemented on a single card, it may be desirable for two or more of those applications to share a single transaction history file. Today's smartcard operating systems do not provide a convenient way to link separate applications to a common transaction history file.

Authentication

Bi-directional verification and authentication between the smartcard and CAD must be provided.

> ***Reason:*** When a card is presented to receive benefit services, the CAD must be able to ascertain whether or not the card is valid before commencing with the transaction. Likewise, there may be some operations where it would be desirable for the card to determine if the CAD is valid.

Blocking Access

The COS should provide the ability to block access to certain files if authentication has not been successfully completed since the last card reset.

Encryption Algorithm

The card operating system must be able to provide DES encryption and decryption.

Message Authentication Codes (MAC)

The COS must be capable of generating and verifying a message authentication code (MAC) on up to 64 bytes of data, based on the DES algorithm, in one uninterrupted operation.

> ***Reason:*** MACs are used to assure the integrity of messages exchanged between the host computer and smartcards. They are calculated by performing a mathematical operation on each character (byte) contained in a message. Then the message and MAC are transmitted together. The receiving party can redo the calculation and compare the result to the accompanying MAC for the purpose of verifying message integrity.

User Authentication

The COS should be able to authenticate a cardholder's identity through the presentation of a valid PIN (personal identification number) or an alternate PIN. All PIN characteristics and rules defined in this document also apply to alternate PINs unless otherwise specified. Both encrypted PINs and PINs in the clear should be supported. If the PIN is not entered properly after a specified number of times in a row, the card must be locked from further use until unlocked in a supervised, secure environment.

> ***Reason:*** Each recipient will select a PIN that must be entered to perform certain transaction types. Recipients may also select an alternate PIN that can be entered instead of the PIN for selected transaction types. For example, an alternate PIN might be assigned to WIC transactions only. This would allow a family member to use the card without having access to all of the functions that might reside on the card.

Card Unlock (PIN)

A secure method must be provided to unlock a card that was previously locked due to improper PIN entry. The card unlock procedure will be performed in supervised secure environment.

Key Replacement

A secure method must be provided to replace the keys that are stored in the card and used by the supported algorithm.

Changing PINs

The COS must support changing keys and PINs by "overwriting" in such a manner that an "unlimited" number of changes are possible throughout the life of the card.

> ***Reason:*** Some COS implementations set aside a fixed amount of memory for storing PIN and key changes. These schemes usually do not overwrite the old value in memory, but instead they establish the new value at a different memory location. When the allotted memory is exhausted, no additional changes can be made.

File Protection

The COS must provide a mechanism for protecting access to files stored in the card's memory based on authorization keys and PINs.

> ***Reason:*** It must be possible to block access to certain information until the proper authorization has been proven, because multiple benefit applications may reside on a single card. Proof will typically be the presentation of password keys, PIN codes, or both.

Rewrite

Rewriting data in the card's memory should be accomplished without requiring a prior "erase" command.

> ***Reason:*** Some card operating systems require a separate erase command to be issued to the card before old data can be replaced with new data.

Integrity of Balance Fields

The COS must accommodate a method to assure the integrity of balance fields stored in the card.

> ***Reason:*** The process of updating balance fields in a card will typically involve the exchange of several commands between the card and CAD, sometimes called a "session." A session could be interrupted prior to normal completion for several reasons, including equipment failure, power failure, or the inadvertent early removal of the card from the CAD.

Logic Extensions and Macros

The COS should be capable of storing programmed logic extensions in Electronically-Erasable Programmable Read-Only Memory (EEPROM). Programmed logic extensions are commands that can be added to the card's memory during chip initialization. These commands become an extension of the card operating system and, once loaded, must be "locked" so they cannot be altered or erased.

> ***Reason:*** The reason for logic extensions is to provide a means to add logic extensions to the COS without rewriting the mask code in the silicon chip. This feature is frequently used to add logic for new and overlooked features.

Reliability

The annualized failure rate for EBT smartcards should be less than 1 percent, excluding user abuse.

Memory Size

The COS should be able to accommodate different application memory sizes without modification to the POS/smartcard command dialogue.

Manufacturer/Supplier Warranty

The manufacturer, vendor, and/or supplier of the technology, systems, services, or products set out in the smartcard procurement warrants and guarantees that:

a. No undisclosed and/or undocumented conditions, functions, or applications exist in any smartcard or other product supplied, that may enable the manufacturer, supplier, or other party to retrieve, obtain, or access any data or programs loaded into the card at any time after manufacture, provided the security features outlined elsewhere in this tender and contained in the product documentation supplied have been employed by the tenderer.

b. All information relating to any physical, logical, program parameters are fully and accurately disclosed in the documentation for the smart card or other product supplied.

c. No features, conditions, functions, or applications of the card relevant to its safe and secure operation are undocumented to the tenderer and/or confidential to the manufacturer or supplier that in any way may affect, degrade, or negate the secure use of the card for its intended purpose.

d. The vendor agrees to replace all cards purchased by the tenderer and to meet all costs associated with replacement, reprogramming, distribution to final users, and any other associated costs should the above conditions (a through c) not be met.

Reason: This provision is intended to ensure that states are fully advised of all features of the cards employed in EBT systems and that a vendor does not have an undisclosed capability to bypass security features of the card and intrude into the privacy of the smartcard user.

GLOSSARY

ACH	Automatic clearing house.
AFDC	Aid to Families with Dependent Children.
Byte	A character; 8 bits.
CAD	Card acceptor device; a hardware device used to read and write information on a smartcard. CADs can be stand-alone devices or incorporated into the design of a terminal or other POS device.
CMS	Card management systems; a hardware and software system used in county offices for card management functions.
COS	Chip or card operating system; a set of instructions permanently burned into the read-only memory (ROM) of a smartcard. Also called a ***mask.*** The instructions usually constitute some primary security and memory management functions.
DES	Data encryption standard. It is a public domain, symmetric, single-key algorithm.
EBT	Electronic benefit transfer; a class of services providing electronic delivery system for government entitlement programs.
EEPROM	Electronically-erasable programmable read-only memory. Allows data to be electronically erased and rewritten.
EMV	Europay, MasterCard and Visa.
FCS	The Food and Consumer Service of the U.S. Department of Agriculture administers the Food Stamp Program and the Special Supplemental Nutrition Program for Women, Infants and Children at the federal level.
FSP	Food Stamp Program.
GA	General Assistance.
Host	Central computer operated by the system vendor to provide core data storage, exchange, and monitoring for the system.
ISO	The International Organization for Standardization.

MAC	Message authentication code; an encrypted value transmitted with all value adding transactions within the PayEase[S.M.] system. The value is calculated using chained DES calculations with keys stored in various components of the PayEase[S.M.] system.
NPC	National City Processing Company, subsidiary of National City Corporation.
PAN	Primary authorization number.
PayEase[S.M.]	EBT system marketed by NPC.
PIN	Personal identification number.
POS	Point of Sale.
Staged Transactions	Transactions generated by the PayEase[S.M.] host computer system that are transmitted to and stored on POS systems for subsequent recording on recipient cards.
USDA	United States Department of Agriculture.
WIC	Special Supplemental Nutrition Program for Women, Infants, and Children.

OVERVIEW OF THE PAYEASE$^{S.M.}$ EBT SYSTEM

The two off-line EBT systems currently in operation in demonstration environments were developed and implemented by the National City Processing Company (NPC).[5] The NPC EBT smartcard system is a subsystem of the NPC EBT PayEase$^{S.M.}$ system. Two components differentiate this subsystem from others: the smartcard and the off-line transaction processing design.

The POS system is designed for use by the general public. No previous technical device operation may be assumed. Retail operation personnel are anticipated to be familiar with retail sales equipment operation, although this may not include stand beside transaction processing equipment as used in the PayEase$^{S.M.}$ operating environment.

The EBT Host provides all EBT processing requirements, including:

- Recipient benefit issuance ("adding value to cards");
- Redemption ("removing value from cards");
- Retail POS and ATM settlement functions;
- Crediting retailer accounts the value of purchases through an Automatic Clearing House (ACH) transaction;
- Drawing-down government accounts for funding the benefits; and
- Strong reporting and auditing processes.

Retailer credit/debit card processing is handled by other NPC departments or service providers.

Bank ATM systems, currency exchange, utility companies, housing authorities, and other POS systems may be incorporated to allow more widespread use and redemption of benefits, as different benefit programs are added to the EBT system.

Card Management Systems (CMS) located at the fiscal control offices of each county provide many card management services, including:

- New card issuance;

[5] Stored Value Systems, a recently-formed subsidiary company of National City Processing Company, has continuing responsibility for the Wyoming EBT demonstration.

- Card diagnostic testing;
- Card replacement;
- Card unlocking; and
- PIN changes.

The CMS also performs a daily host settlement in the same manner as do the retail POS system locations.

All authorized recipients carry a PayEase$^{S.M.}$ smartcard. The card retains records of the available benefit amount and a history file of benefit transactions.

Potential recipients contact the proper government aid caseworker for certification as an entitlement program recipient.

Eligible recipient information is input into the states aid certification system by the caseworker and transmitted to the host.

A PayEase$^{S.M.}$ smartcard is then issued to eligible recipients using the county CMS, during which time certain information in the card is personalized, including:

- A primary PIN;
- An alternate PIN; and
- Up to three participating retail locations selected by the recipient for benefit pickup.

Value is not added to the card at the CMS. For security considerations, recipient setup information is transmitted to the host, which creates records concerning benefit levels and availability. Those records trigger the off-line replenishment process, which creates a staged transaction for adding value. During the daily settlement process, staged transactions are transmitted from the host to the proper retail POS locations previously selected by the recipient (up to three for each card).

Recipients can then use their PayEase$^{S.M.}$ smartcards at any of the retail locations they selected to receive their benefits through the off-line replenishment process. Once a recipient's card is loaded, it can then be used to make purchases at any program participating retailer.

One of the key features in the EBT solution provided by NPC is the ability to perform a remote, off-line replenishment of a benefit recipient's card. Off-line replenishment is the

mechanism used for automatically updating a recipient's card with initial and ongoing benefits after they are authorized by the issuing agency. This is accomplished by having the POS platform maintain a database of issuance benefit records. Each benefit record is keyed to a specific recipient card by a Primary Authorization Number (PAN). When the issuing agency notifies the EBT host of an available benefit for a recipient, a record is created and distributed to the POS network detailing this benefit (staged transactions). These records contain the PAN, the benefit amount, beginning and ending benefit available dates, a host-generated reference number used for tracking the benefit, and a MAC used to certify that the record's contents were not compromised during message transmission.

An important issue in the off-line replenishment process is insuring that the recipient balance is not updated at multiple locations. This is because each value-adding benefit transaction is distributed to up to three retail POS locations. Protection from multiple updates is being satisfied by searching the card's transaction history file before adding value to the proper balance field. If the record is found, it is not posted again. If the record is not found, the proper balance field is updated and the record is added to the card's history file. In either case, an acknowledgment record is saved by the POS system and returned to the host, thus indicating the benefit has been posted to the card.

The host updates its database when acknowledgment records are received from the POS system. Thereafter, any POS system performing a settlement session with the host will receive a database delete command to remove posted transactions from the POS database. This feature helps ensure that old transactions do not remain in the POS systems database, and reduces the time required to search staged transaction databases by minimizing their contents.

The off-line replenishment algorithm requires a circular history file and the ability to block card use when that file is filled with transactions that all occurred within the last seven days. Staged transactions are transmitted to up to three selected retail locations, where they await the recipient's card. The card is updated and the transaction is added to the history file the first time the card is presented at any of the selected retail locations. The retail POS system where the card was updated sends an acknowledgment during its next settlement session with the host. The host updates its database and sends a delete record to the other two retail locations during subsequent settlement sessions.

The normal length of time to remove an acknowledged transaction is two to three days. During that time, if the card is presented at the other selected retail locations it will not be updated as long as the transaction is contained in the card's history file. Therefore, if the circular history file is full and old transactions are being replaced, only transactions that are greater than seven days old may be overwritten. Otherwise, multiple updates might occur. In the event a cardholder attempts to perform more transactions in a week than the card can maintain in its history file, those transactions will not be authorized. As soon as the transactions age to seven days, additional transaction activity is allowed. The number of days provided by this check needs to be an input parameter to the COS at card initialization or personalization time. The value will depend on the amount of history file space available on the card, and will vary depending on total card memory capacity.

Benefits, other host-staged transactions, and purchases are posted to the smartcard transaction storage area as they occur. Purchase transactions deduct the value of the purchase from the proper benefit balance (electronic purse) carried in the smartcard.

The MAC accompanying a transaction from the host must be verified before the transaction is posted to the card to ensure the transaction has not been compromised. To simplify and secure this process, the card should be capable of performing these operations in one uninterrupted operation. In addition, this operation should be constructed so that attempts to breach system security will be thwarted. This includes altering the voltage, clock or other physical interconnects, or other mechanisms. The process of posting value to a card must ensure that the proper balance in the card is incremented or decremented by the indicated amount.

When a food stamp transaction is processed, the recipient's card must be decremented by the purchase amount, a history record stored on the card containing the transaction details, and an acknowledgment record stored on the retail POS, which is returned to the host during settlement. When the COS posts a transaction to the card it must generate a MAC certificate. This certificate is attached to the acknowledgment record to ensure the data is processed throughout the system without modification. This requires the selection and use of the proper security key(s). Placing this operation in control of the card minimizes the distribution of issuer keys to third parties, and thus helps to protect the entire EBT system. High value commercial transactions will likely require this type of capability.

Transactions involving WIC balance fields are further impacted by this program's item-specific nature. The recipient account balance contains authorized levels of purchase, for example, quarts of milk cans of juice, etc. The retailer is concerned only with remittance of the appropriate dollar value of this transaction, however. The card is actively involved in meeting these requirements. The transaction update command identified for the card should have the capacity to pass several account balances, as well as identifying an overall dollar value with this transaction. The various account balances must be adjusted in a fashion that ensures the balance fields and history file are updated properly. In addition, an overall record must be formatted and written to the card's history file that adheres to a standard transaction record format. The input command may be structured to force the POS to provide both types of information to the card in the same command. The card should still be responsible, however, for generating a MAC certificate to accompany the dollar value of the transaction throughout the financial networks involved in settling this transaction to the retailer's account.

Some of the issues that should be resolved include the ability to:

- Identify the elements of a transaction message that are used in the MAC calculation;
- Identify the elements of a transaction message used to determine if the transaction was previously posted to the card; and
- Extend the posting process to include incrementing or decrementing multiple balance fields with one command.

Staged transactions will be the likely mechanism for applying refunds, manual transactions approved when a POS is inoperative, and card-adjusting transactions required by state or operating agencies. Therefore, both debit and credit transactions must be supported.

A possible input component to this operation may be requiring the POS to indicate to the card which program (purse) balance fields may be impacted during a transaction. Based on this, the card may access additional fields in the input command parameters and file headers to determine how the search operation should be conducted when determining if the card has already been updated with this transaction. This would imply a security mechanism that is associated with the indicated balance field, in addition to the transaction history file.

Records indicating staged transactions, purchases, and other activities are recorded by the POS system and transmitted to the host. The process of uploading EBT POS transaction

records from the POS system to the host, and receiving downloaded staged transactions from the host to the POS, is commonly referred to as a "host settlement." The transaction purchase values are credited to the retailer's bank account via an ACH deposit transaction. The entitlement value is debited from state and federal accounts using established ACH transfers.

The principal interfaces for the smartcard are the POS system and the county CMS. This includes any system with POS functionality, such as ATMs used to withdraw cash from cash valued entitlement benefit programs, or other service providers that are authorized to accept government benefit payment options.